



TRENDnet



User's Guide

TEW-430APB

Regulatory notes and statements

Wireless LAN, Health and Authorization for use

Radio frequency electromagnetic energy is emitted from Wireless LAN devices. The energy levels of these emissions however are far much less than the electromagnetic energy emissions from wireless devices like for example mobile phones. Wireless LAN devices are safe for use frequency safety standards and recommendations. The use of Wireless LAN devices may be restricted in some situations or environments for example:

- On board of airplanes, or
- In an explosive environment, or
- In case the interference risk to other devices or services is perceived or identified as harmful

In case the policy regarding the use of Wireless LAN devices in specific organizations or environments (e.g. airports, hospitals, chemical/oil/gas industrial plants, private buildings etc.) is not clear, please ask for authorization to use these devices prior to operating the equipment.

Regulatory Information/disclaimers

Installation and use of this Wireless LAN device must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications made to this device that are not expressly approved by the manufacturer may void the user's authority to operate the equipment. The Manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device, of the substitution or attachment. Manufacturer and its authorized resellers or distributors will assume no liability for any damage or violation of government regulations arising from failing to comply with these guidelines.

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause

harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

We declare that the product is limited in CH1~CH11 by specified firmware controlled in the USA.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.



TABLE OF CONTENT

About This Guide	1
Purpose.....	1
Overview of this User's Guide	1
Unpacking and Setup.....	2
Unpacking.....	2
Setup	2
Hardware Installation.....	3
Front panel	3
Rear Panel	3
Hardware connections	4
Connect to the Switch/Hub	4
Check the installation.....	4
Configuring the Wireless LAN Access Point.....	6
Login to the Wireless AP through WLAN	6
Login.....	6
Main Screen of the Access Point.....	7
Wizard.....	8
Status.....	10
Basic Setting	12
Access Point Mode	12
AP Client mode.....	15
WDS mode.....	18
AP+WDS mode	22
Repeater mode	23
IP Setting	26
Advanced Setting.....	27
Security	28
Tools	29
Technical Specifications.....	30

ABOUT THIS GUIDE

Congratulations on your purchase of this IEEE 802.11g Wireless LAN Access Point. This manual helps to features the innovating wireless technology that can help you build a wireless network easily! This manual contains detailed instructions in operation of this product. Please keep this manual for future reference.

With a WLAN (IEEE 802.11g) Access Point, a mobile computer can share data with another mobile computer in a wireless way. Easy-to-use utilities are bundled with WLAN Access Point for configuration and monitoring purposes.

WLAN networking can wirelessly transmit and receive data, minimizing the need for wired connections, at a speed of up to Fifty-four megabit per second. With WLAN networking, you can locate your PC wherever you want without wires and cables.

WLAN networking provides users with an access to real-time information anywhere in their organization. The mobility provides productivity and service, which are not available under wired networks.

Purpose

This manual discusses how to install the WLAN Access Point.

Overview of this User's Guide

Introduction. Describes the WLAN Access Point and its features.

Unpacking and Setup. Helps you get started with the basic installation of the WLAN Access Point.

Hardware Installation. Describes the LED indicators of the AP.

Software Installation. Tells how to setup the driver and the utility setting.

Technical Specifications. Lists the technical (general, physical and environmental) specifications of the WLAN Access Point.

UNPACKING AND SETUP

This chapter provides unpacking and setup information for the Access Point.

Unpacking

Open the box of the Access Point and carefully unpack it. The box should contain the following items:

- ◆ One Wireless Access Point
- ◆ One external power adapter
- ◆ One Multi-Language Quick Installation Guide
- ◆ One CD-Rom (User's guide)

If any item is found missing or damaged, please contact your local reseller for replacement.

Setup

The setup of the Wireless Access Point can be performed using the following steps:

- ◆ Locate an optimum location for the Wireless LAN Access Point (AP). The best place for your AP is usually the center of your wireless network, with line of sight to all of your mobile stations.
- ◆ Visually inspect the Ethernet RJ45 port connector and make sure that it is fully plugged in to the system's Ethernet switch/hub port.
- ◆ Fix the direction of the antennas. Try to place the AP in a position that can best cover your wireless network. Normally, the higher you place the antenna, the better the performance will be. The antenna's position enhances the receiving sensitivity.
- ◆ Visually inspect if the Power Adapter was fully plugged to the device power jack.

HARDWARE INSTALATION

Front panel

The figure below shows the LED Indicator of the Wireless LAN Access Point.



WLAN:

The indicator blinking green whiles the wireless LAN activity.

LAN (Link/ACT):

The indicator lights green when the LAN port is connected to a Ethernet network successful. Otherwise, the indicator blinking green while transmitting or receiving data on the Ethernet network.

Rear Panel

The figure below shows the rear panel of the Access Point



LAN

Ethernet port with 10/100Mbps Fast Ethernet connections, connect this port to switch/hub.

RESET

The Reset function is to reset the setting back to factory default setting, once you press the “RESET” button more than 5 seconds.

Power

Connect the Power Adapter DC plug to the AP's power jack.

Antenna

One external dipole antenna.

Hardware connections



Connect to the Switch/Hub

1. Plug in one end of the RJ45 network cable to the Switch/Hub port,
2. Plug in the other end of the RJ45 network cable to the Wireless Access Point.

Check the installation

The LEDs of the Access Point are clearly visible and the status of the network link can be seen instantly:

1. With the power source on, once the device is connected, the Power, LAN and WLAN port LEDs will light up indicating a normal status.

2. If the LAN Port's Link indicator does not light up then check the RJ-45 cable if it is firmly feed to the RJ45 port, while the LAN is link up to the Switch/Hub, the LAN port's LED will light up.

CONFIGURING THE WIRELESS LAN ACCESS POINT

The Wireless Access Point has a Web GUI interface for the configuration. The AP can be configured through the Web Browser. A network manager can manage, control and monitor the AP from the local LAN. This section indicates how to configure the AP to enable its functions.

Login to the Wireless AP through WLAN

Before configuring the Wireless AP through WLAN, make sure that the SSID, Channel and the WEP was set properly.

The default setting of the Wireless AP that you will use:

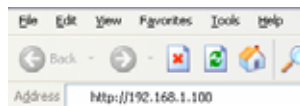
- ◆ SSID: TRENDnet
 - ◆ Channel: 6
 - ◆ WEP Encryption: disable
 - ◆ IP address: 192.168.1.100
-

Login

Before you configure this device, note that when the AP is configured through an Ethernet connection, make sure the manager PC must be set on same the **IP network**. For example, when the default network address of the default IP address of the AP is **192.168.1.100**, then the manager PC should be set at 192.168.1.x (where x is a number between 2 and 254), and the default subnet mask is 255.255.255.0.

Open Internet Explorer 5.0 or above Web browser.

Enter IP address ***http://192.168.1.100*** (the factory-default IP address setting) to the address location.



When there is a screen needs to enter the User name and Password, both of the default Username and Password is “admin”



Main Screen of the Access Point

The screen will show the status of the AP when you login to the AP.

There are seven main functions: Wizard, Status, Basic Setting, IP Setting, Advanced Setting, Security and Tools.



Wizard

Setup wizard is provided as the part of the web configuration utility. User can simply follow the step-by-step process to get Access Point configuration ready to run in 4 easy steps by clicking on the **“Wizard”** button on the function menu. The following screen will appear. Please click **“Next”** to continue.



Step 1: Set Password

User can change the password and then click **“Next”** to continue.



Step2: Set WLAN Connection

Please type the name of SSID and select the Channel. Then, click **“Next”** to continue.



Step 3: Set WEP Encryption

If user wants to enable WEP, please click **“Enabled”**. Then, select the key size of WEP encryption and enter the key value in the key text box. Please click **“Next”** to continue.



Step 4: Restart

The Setup wizard is now completed. The new settings will be effective after the Access Point restarted. Please click **“Restart”** to reboot the Access Point. If user does not want to make any changes, please click **“exit”** to quit without any changes. User also can go back to modify the setting by clicking **“back”**.



Status

This page as below shows the following information.



Firmware Version: Shows the current firmware version and released date code.

LAN: Shows the Mac address, IP address (default: 192.168.1.100), Subnet Mask, Gateway Address. The current LAN traffic calculated in terms of number of packets sent and received by AP through wired connection is also displayed.

Wireless: Shows the Mac address, current SSID, the status of Encryption Function (Enable or Disable), the current using channel. The current wireless traffic calculated in terms of number of packets sent and received by AP through wireless communication is also displayed.

View Log: Once clicked, the page will change to login page. The login page records every event and the time that it happens.



User may clear the entries recorded in the log by clicking the “Clear Log” button, and refresh the screen to show the latest log entries by clicking the “Refresh” button.

Basic Setting

This is the page allow user to change the access point settings.

The screenshot shows the 'Basic Setting' page for a TRENDnet 54Mbps 802.11g Wireless Access Point (TEW-430APB). The page has a sidebar with navigation buttons: Wizard, Status, Basic Setting (selected), IP Setting, Advanced Setting, Security, and Tools. The main content area is titled 'Basic Setting' and includes a 'HELP' button. The settings are as follows:

- AP Name:** 802.11g Wireless LAN
- Mode:** Access Point (dropdown menu)
- Channel:** 6 (dropdown menu)
- SSID:** TRENDnet (text input field) with a 'Site Survey' button next to it.
- Authentication:** Radio buttons for Open System (selected), Shared Key, WPA-PSK, WPA2-PSK, WPA, and WPA2.
- WEP Key:** Radio buttons for Enabled and Disabled (selected).

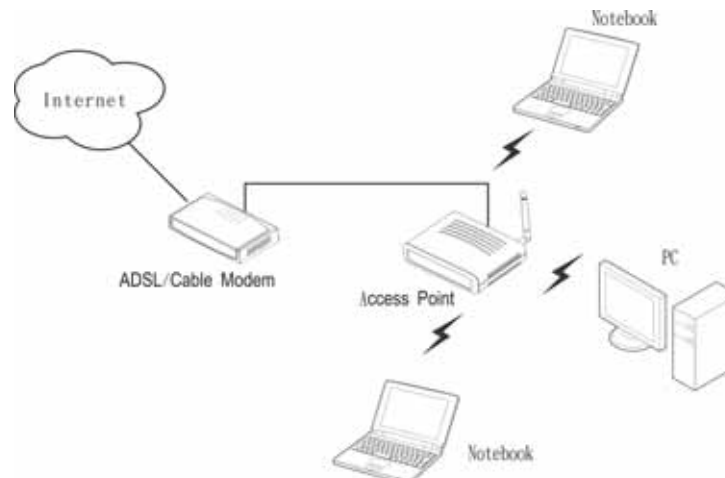
At the bottom of the settings area are 'Apply' and 'Cancel' buttons. A copyright notice at the bottom right reads: 'Copyright © 2006 TRENDnet. All Rights Reserved.'

AP Name: The name of the AP, which can be used to identify the Access Point among the all the Access Points in the wireless network.

Mode: The WLAN AP supports five operation mode for Access Point, AP Client, WDS (Wireless Distribution System), AP+WDS and Repeater mode.

Access Point Mode

Configure the AP to Access Point mode; with this mode, WLAN clients can access LAN or other WLAN clients through this AP.



AP mode application

The screenshot shows a configuration window for an Access Point. The fields are as follows:

- AP Name:** 802.11g Wireless LAN
- Mode:** Access Point (dropdown menu)
- Channel:** 5 (dropdown menu)
- SSID:** TRENDnet (text input field) with a **Site Survey** button next to it.
- Authentication:** Open System (selected with a radio button), Shared Key, WPA-PSK, WPA2-PSK, WPA, and WPA2 (all unselected).
- WEP Key:** Enabled (unselected) and Disabled (selected with a radio button).
- At the bottom, there are **Apply** and **Cancel** buttons.

AP mode configuration

Channel: The channel that AP will operate in. User can select the channel range from 1 to 11 for North America (FCC) domain, 1 to 13 for European (ETSI) domain and 1 to 14 for Japanese domain.

SSID: Service Set Identifier, which is a unique name shared among all clients and nodes in a wireless network. The SSID must be identical for each clients and nodes in the wireless network.

Authentication Type: The authentication type default is set to Open system. There are six options: Open system; Shared Key; WPA-PSK, WPA2-PSK, WPA and WPA2. User may want to set to Shared Key when the clients and AP in the same wireless network enable the encryption. All the nodes and hosts on the network must use the same authentication type.

WEP Key: To disable WEP security, click on the “Disable” option. To enable WEP security, there are 2 types to select – 64bits and 128 bits. When it is selected, the key value must be entered in ASCII or HEX format.

Note: When the WEP security is enabled, all the wireless clients that wish to connect to the Access Point must also have WEP enabled with the identical WEP Key value entered.



WPA-PSK / WPA2-PSK:

If WPA-PSK or WPA2-PSK is selected, user needs to set the key in the passphrase field as the below screen. The key length should be 8 characters at least.



WPA / WPA2:

If WPA or WPA2 is selected, the below screen is shown. Please set the length of the encryption key and the parameters for the RADIUS server.



RADIUS Server 1:

Enter the IP address of and the Port used by the Primary Radius Server, enter the Shared Secret, which is used by the Radius Server.

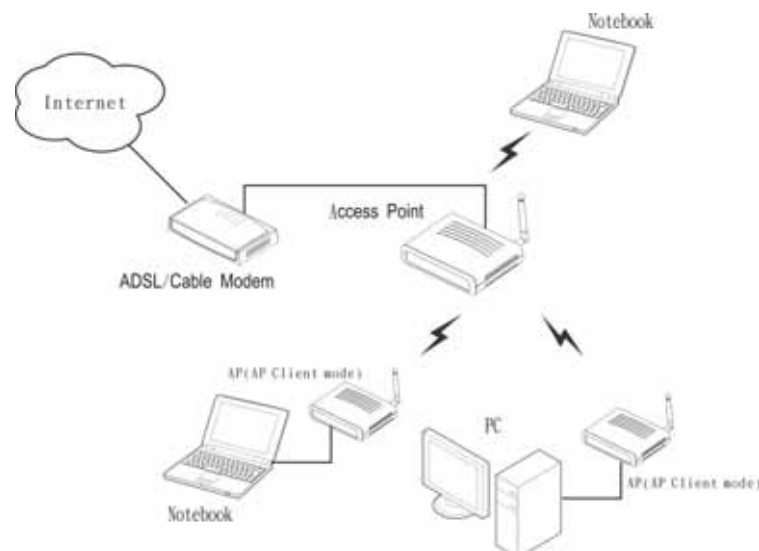
RADIUS Server 2: (optional)

Enter the IP address of and the Port used by the Secondary Radius Server, enter the Shared Secret, which is used by the Radius Server.

Apply: For the changes made to any of the items above to be effective, click “Apply”. The new settings are now been saved to Access Point and will be effective once the Access Point restarts.

AP Client mode

Configure the AP to AP Client mode; the AP will be a wireless Ethernet adapter transforms any Ethernet-enabled devices to have the wireless function.



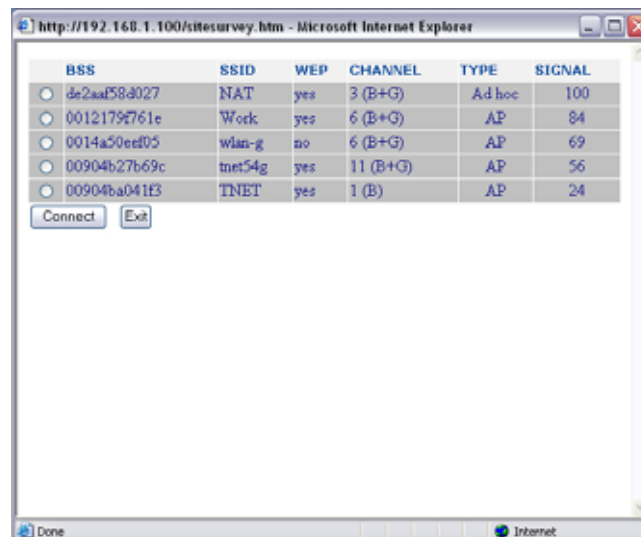
AP Client mode application

AP Name:	802.11g Wireless LAN	
Mode:	AP Client	
Channel:	6	
SSID:	TRENDnet	Site Survey
Authentication:	☒ Open System ☐ Shared Key ☐ WPA-PSK ☐ WPA2-PSK ☐ WPA ☐ WPA2	
WEP Key:	☐ Enabled ☒ Disabled	
Apply Cancel		

AP Client mode configuration

SSID: Service Set Identifier, which is a unique name shared among all clients and nodes in a wireless network. The SSID must be identical for each clients and nodes in the wireless network.

Site Survey: This button allows user to enable the Site Survey function to scan for the available wireless network (wireless clients and Access Points) and establish wireless communications with one. Selected one of them in list to establish communications and click “Connect” button.



Authentication Type: The authentication type default is set to Open system. There are four options: Open system; Shared Key; WPA-PSK and WPA2-PSK. User may want to set to Shared Key when the clients and AP in the same

wireless network enable the WEP encryption. All the nodes and hosts on the network must use the same authentication type.

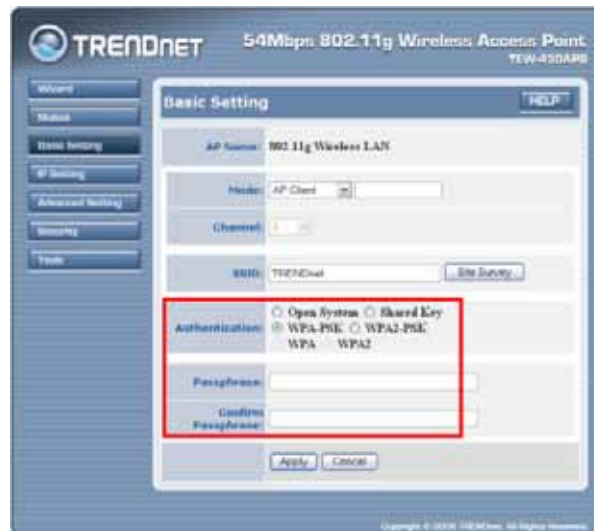
WEP Key: To disable WEP security, click on the “Disable” option. To enable WEP security, there are 2 types to select – 64bits and 128 bits. When it is selected, the key value must be entered in ASCII or HEX format.

Note: When WEP security is enabled, all the wireless clients that wish to connect to the Access Point must also have WEP enabled with the identical WEP Key value entered.



WPA-PSK / WPA2-PSK:

If WPA-PSK or WPA2-PSK is selected, user needs to set the key in the passphrase field as the below screen. The key length should be 8 characters at least.



Apply: For the changes made to any of the items above to be effective, click “Apply”. The new settings are now been saved to Access Point and will be effective once the Access Point restarts.

Note: For entering to the Web Setting page after changing to AP Client mode, change your PC/Notebook IP address to 192.168.1.x. After changing your IP address, type 192.168.1.100 on the Web browser to enter the setting of this Wireless AP.

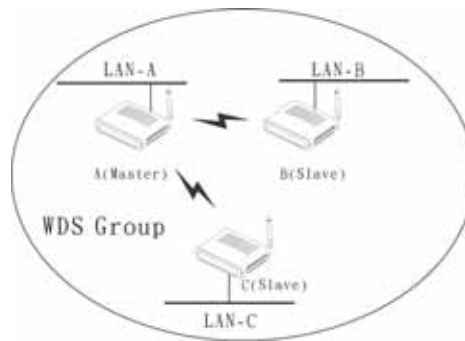
WDS mode

With WDS (Wireless Distribution System) mode, user can use wireless media to communicate two or more LANs through the AP with WDS mode, all of the LAN will be combined in the WDS group, for example:

Single WDS group application:

When there are three APs joined to the WDS group, one of the AP in WDS mode will be the Master, the other two APs will be the Slave, all of the APs in the WDS group must use the same wireless channel and the same security setting, the Master need to fill all the Slave’s MAC address in the “Remote AP Mac” list, and the Slave need to fill the Master’s MAC address in the “Remote AP Mac” list, the maximum of one Master can join eight Slave to be one WDS group.

In this example, LAN-A can communicate with LAN-B and LAN-C, and LAN-B can communicate with LAN-C through the AP-A. All of LANs will be at the same LAN environment coming through LAN-A.



WDS mode application (Single WDS group)

Master setting (AP-A)

Slave setting (AP-B and AP-C)

WDS mode configuration for Example-1

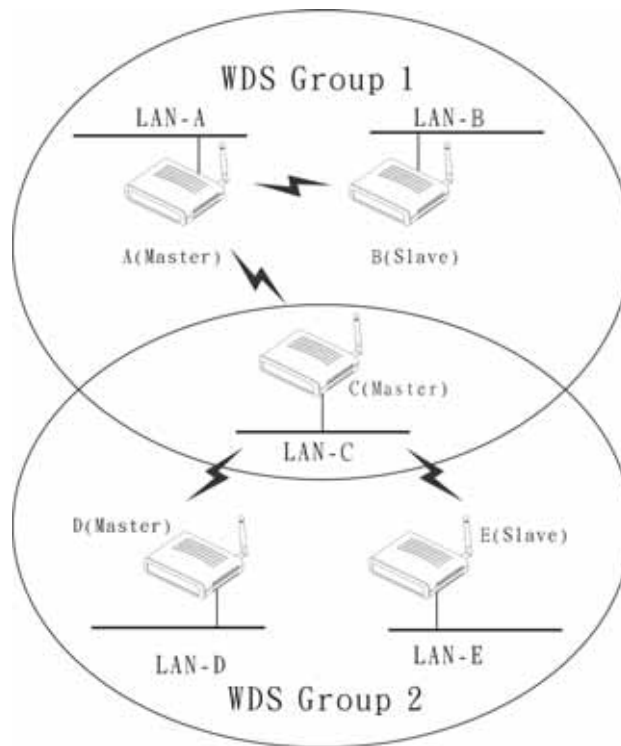
Multiple WDS group application:

When there are five APs to be join into two separated WDS group, the member of WDS group 1 is AP-A, AP-B and AP-C, and member of the WDS group 2 is AP-C, AP-D and AP-E, the AP-C will join both of WDS group 1 and WDS group 2, each WDS Group 1 will be one master and the other will be slave.

The AP-A and AP-C will be both as a Master AP for both WDS Groups, the AP-A represent for the master of WDS Group 1, the AP-C represent for the master of the WDS Group 2 and at the same time AP-C will be the slave of WDS Group 1, so all of the APs in the two WDS groups must use the same wireless channel and same security, the Master need to fill all of Slave's MAC address in the "Remote AP Mac" list, and the Slave need to fill the Master's MAC address in the "Remote AP Mac" list, maximum allow one Master can be join eight Slaves to be one WDS group.

In this example, LAN-A can communicate with LAN-B and LAN-C, and LAN-B can communicate with LAN-C through the AP-A. LAN-B will have the same LAN environment coming through LAN-A.

LAN-E can communicate with LAN-B and LAN-D, LAN-E can communicate with LAN-D through AP-C, LAN-E can communicate with LAN-B through AP-C and AP-A, LAN-E will have the same LAN environment coming through LAN-A.



WDS mode application (Multiple WDS group)

The image displays two side-by-side screenshots of a web interface for configuring WDS mode. Both screens are titled 'Basic Setting' and have a 'HELP' button in the top right corner. The 'AP Name' is set to '802.11g Wireless LAN'. The 'Mode' is set to 'WDS' and the 'Channel' is set to '6'.
 The left screenshot is for a Master setting (AP-A, WDS Group 1). It shows 'Remote AP Mac' with two fields: '1. MAC address of AP-B' and '2. MAC address of AP-C'. Below these are four more empty fields for additional MAC addresses. The 'WDS Security' is set to 'none', and there are fields for 'WEP Key' and 'Passphrase (0-63 char.)'. 'Apply' and 'Cancel' buttons are at the bottom.
 The right screenshot is for a Slave setting (AP-B, WDS Group 1). It shows 'Remote AP Mac' with two fields: '1. MAC address of AP-A' and '2. MAC address of AP-C'. Below these are four more empty fields for additional MAC addresses. The 'WDS Security' is set to 'none', and there are fields for 'WEP Key' and 'Passphrase (0-63 char.)'. 'Apply' and 'Cancel' buttons are at the bottom.

Master setting (AP-A, WDS Group 1)

Slave setting (AP-B, WDS Group 1)

Basic Setting

HELP

AP Name: 902.11g Wireless LAN

Mode: WDS

Channel: 6

Remote AP Mac:

1: MAC address of AP-A

2: MAC address of AP-D

3: MAC address of AP-E

4:

5:

6:

7:

8:

WDS Security: none

WEP Key:

Passphrase: (0-63 char.)

Apply

Cancel

Basic Setting

HELP

AP Name: 902.11g Wireless LAN

Mode: WDS

Channel: 6

Remote AP Mac:

1: MAC address of AP-C

2:

3:

4:

5:

6:

7:

8:

WDS Security: none

WEP Key:

Passphrase: (0-63 char.)

Apply

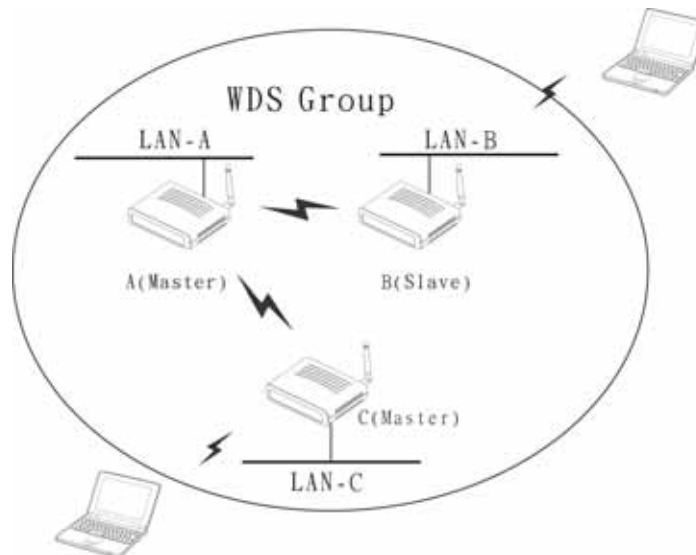
Cancel

Master setting (AP-C, WDS Group 2) Slave setting (AP-D and AP-E, WDS Group 2)

WDS mode configuration for Example-2

AP+WDS mode

With WDS+AP mode, user can use wireless media to communicate two or more LANs through the AP with WDS+AP mode, all of LAN will be combined in the WDS group and WLAN client can access to the AP with AP+WDS mode.



WDS+AP mode application

AP Name:	802.11g Wireless LAN	
Mode:	AP+WDS	
Channel:	6	
SSID:	TRENDnet Site Survey	
Authentication:	☐ Open System ☐ Shared Key ☐ WPA-PSK ☒ WPA2-PSK ☐ WPA ☐ WPA2	
Passphrase:		
Confirm Passphrase:		
Remote AP Mac:	1. 2. 3. 4. 5. 6. 7. 8.	
WDS Security:	WEP 64bits	
WEP Key:	ASCII	
Passphrase: (8~63 char.)		

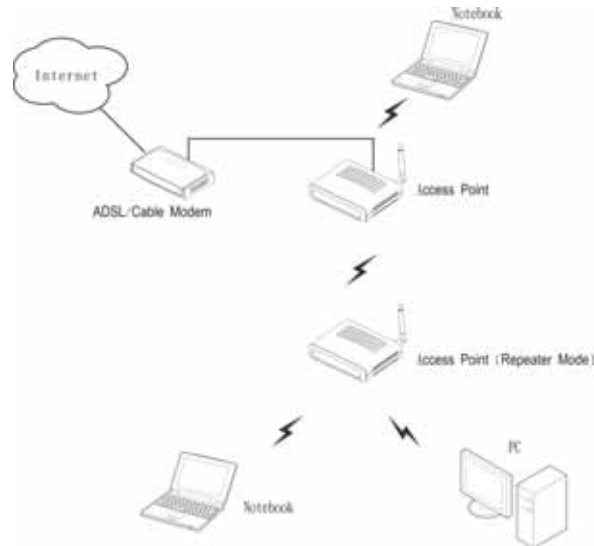
AP configuration

WDS configuration

Please refer the AP mode and WDS mode for detail configuration.

Repeater mode

Configure the AP to Repeater mode; the AP will be a wireless LAN repeater that will be extended the WLAN coverage range.



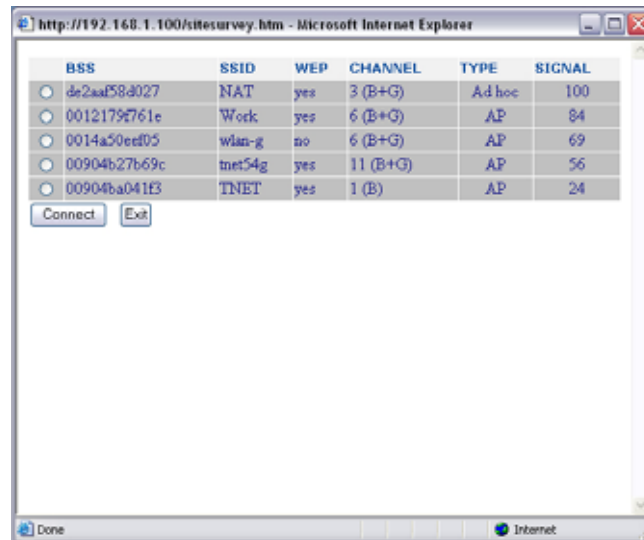
Repeater mode application

AP Name:	802.11g Wireless LAN	
Mode:	Repeater	
Channel:	6	
SSID:	TRENDnet	Site Survey
Authentication:	☒ Open System ☐ Shared Key ☐ WPA-PSK ☐ WPA2-PSK ☐ WPA ☐ WPA2	
WEP Key:	☐ Enabled ☒ Disabled	
Apply Cancel		

Repeater mode configuration

SSID: Service Set Identifier, which is a unique name shared among all clients and nodes in a wireless network. The SSID must be identical for each clients and nodes in the wireless network.

Site Survey: This button allows user to enable the Site Survey function to scan for the available wireless network (wireless clients and Access Points) and establish wireless communications with one. Selected one of them in list to establish communications and click “Connect” button.



Authentication Type: The authentication type default is set to Open system. There are four options: Open system; Shared Key; WPA-PSK and WPA2-PSK. User may want to set to Shared Key when the clients and AP in the same wireless network enable the WEP encryption. All the nodes and hosts on the network must use the same authentication type.

WEP Key: To disable WEP security, click on the “Disable” option. To enable WEP security, there are 2 types to select – 64bits and 128 bits. When it is selected, the key value must be entered in ASCII or HEX format.

Note: When WEP security is enabled, all the wireless clients that wish to connect to the Access Point must also have WEP enabled with the identical WEP Key value entered.



WPA-PSK / WPA2-PSK:

If WPA-PSK or WPA2-PSK is selected, user needs to set the key in the passphrase field as the below screen. The key length should be 8 characters at least.



The screenshot shows a web-based configuration interface for a wireless router. The 'AP Name' is '802.11g Wireless LAN'. The 'Mode' is set to 'Repeater'. The 'Channel' is '11'. The 'SSID' is 'TrendNet'. The 'Authentication' section is highlighted with a red box and contains the following options: 'Open System', 'Shared Key', 'WPA-PSK' (selected), 'WPA2-PSK', 'WPA', and 'WPA2'. Below the authentication options are fields for 'Passphrase', 'Confirm Passphrase', and 'Apply' and 'Cancel' buttons.

Apply: For the changes made to any of the items above to be effective, click “Apply”. The new settings are now been saved to Access Point and will be effective once the Access Point restarts.

IP Setting

This page allows user to configure the IP and DHCP settings of the Access Point.

The screenshot shows the web interface of a TRENDnet 54Mbps 802.11g Wireless Access Point (TEW430APB). The 'IP Setting' page is displayed, featuring a sidebar with navigation links: 'Wizard', 'Status', 'Basic Setting', 'IP Setting' (selected), 'Advanced Setting', 'Security', and 'Tools'. The main content area contains the following settings:

- LAN IP:** Radio buttons for 'Obtain IP Automatically' and 'Fixed IP'. 'Fixed IP' is selected.
- Address:** Text box containing '192.168.1.100'.
- Subnet Mask:** Text box containing '255.255.255.0'.
- Gateway:** Text box containing '0.0.0.0'.
- DHCP Server:** Radio buttons for 'On' and 'Off'. 'Off' is selected.
- IP Range:** 'From' text box contains '192.168.1.101' and 'to' text box contains '192.168.1.200'.
- DNS Server:** Empty text box.

At the bottom of the form are 'Apply' and 'Cancel' buttons. A 'HELP' button is located in the top right corner of the settings area. The footer of the page reads 'Copyright © 2006 TRENDnet. All Rights Reserved.'

The default IP address of this access point is 192.168.1.100 with the subnet mask of 255.255.255.0. User can type in other values for IP Address, Subnet Mask and Gateway and click “**Apply**” button for the changes to be effective.

User can also set the Access Point to obtain the IP from a DHCP server, but it is not recommended. Select the option “Obtain IP Automatically” and click “**Apply**” button for the changes to be effective.

DHCP Server: It is not recommended to enable the DHCP Server if user has a DHCP server running in LAN network because it probably will cause possible the conflict of IP assignment. Enable the DHCP server function by selecting the option “**On**”, and enter the IP range.

DNS Server: Type up to DNS IP address in the text boxes. Your ISP will provide you with this information.

Click “**Apply**” for the changes to be effective

Advanced Setting

This page contains configurations for advanced users, which the change reflects the wireless performance and operating modes.



Beacon Interval: To set the period of time in milliseconds that AP sends out a beacon. Default is 100 milliseconds.

RTS Threshold: To set the size of RTS/CTS packet size. Default is 2432 bytes.

Fragmentation Threshold: To set the number of bytes used for the fragmentation boundary for directed messages. Default is 2436 bytes.

DTIM Interval: This value indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the access point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM interval value. Access point clients hear the beacons and awaken to receive the broadcast and multicast messages.

SSID Broadcast: While SSID Broadcast is enabled, all wireless clients will be able to communicate with the access point. For secure purpose, user may want to disable SSID broadcast to allow only those wireless clients with the AP SSID to communicate with the access point.

Mode Setting: To setting the AP operation mode for 802.11g only or 802.11b/802.11g mix mode

TX Rates: Select one of the wireless communications transfer rates, measured in megabytes per second, based upon the speed of wireless adapters connected to the WLAN.

Security

This page is where user configures the security features supported by this Access Point.



Password: Allow user to change the new login password. Here are the necessary steps:

1. Enter the new password in the “**AP Password New:**” field.
2. Enter the new password again in the “**Confirm**” field.
3. Click “**Apply**”

MAC Filter: MAC Filter function controls the MAC of the network devices that are listed in this table for access authorization or denial. There have three choices:

- ◆ Disable MAC Filters
- ◆ Only **allow** PCs with MAC listed below to access device
- ◆ Only **deny** PCs with MAC listed below to access device

The maximum number of MAC addresses that can be stored is 50. User can browse through the MAC address saved by selecting the MAC Filter List.

For any changes made in the security page, click “Apply” for the changes to be effective.

Tools

Four functions are provided in this page, Backup, Restore Settings, Restore default settings and Firmware Upgrade.



Save Settings to Local Hard Drive: Click on “**Save Settings to Local Hard Drive**” button, which will open a FileSave Dialog box, where user gets to save all the current settings and configurations to a file.

Restore Settings: Click on the “**Browse**” button to open a FileOpen Dialog box, where user gets to select the file, which saves previous settings and configurations. Upon selecting the saved file, click “**Restore**” and complete the restore process when the access point re-operates after it restarts.

Restore to default settings: Click on “**Default**” button to restore the access point back to its manufacture default settings.

Firmware Upgrade: Click on the “**Browse**” button to open a FileOpen Dialog box, where gets to select the firmware file, which download from the web for the latest version. Upon selecting the firmware file, click “**Upgrade**” and complete the firmware upgrade process when the Access Point re-operates after it restarts.

TECHNICAL SPECIFICATIONS

General	
Standards	IEEE 802.11b/g IEEE 802.3u 10/100BASE-TX Fast Ethernet
Signal Type:	DSSS (802.11b) OFDM (802.11g)
Modulation:	QPSK / BPSK / CCK / OFDM
LED Indicators:	Power, LAN (Link/Activity), WLAN (Link)
Frequency	2412 MHz ~ 2462 MHz (FCC) 2412 MHz ~ 2472 MHz (ETSI) 2400 MHz ~ 2484 MHz (Japan)
Channel	1~ 14 Channels *Local Regulatory Restrictions May Apply.
Data Encryption:	64 bit / 128 bit WEP Encryption, WPA, WPA2, WPA-PSK, WPA2-PSK
Data Transfer Rate	Fast Ethernet: 10/100Mbps Wireless: Up to 54Mbps (with Automatic Scale Back)
Receiver Sensitivity	54Mbps: Typical -68 dBm @10% PER 11Mbps: Typical -81 dBm @8% PER
Transmit Power	802.11g: Minimum 13dBm typically 802.11b: Minimum 15dBm typically
Transmission Range:	Outdoor: 100~300M (depends on environment) Indoor: 50~100M (depends on environment)
Network Cables	2-pair UTP/STP Cat. 3,4,5 (100 m)
Interface	1 x 10/100Mbps RJ45 port
Antenna:	1 x 2 dBi Dipole Antenna
Physical and Environmental	
DC inputs	DC 7.5V /1A

Power Consumption	4.2W (Max)
Temperature	Operating: 0 ~ 40 °C, Storage: -10 ~ 70 °C
Humidity	Operating: 10% ~ 90%, Storage: 5% ~ 90%
Dimensions	140 x 98 x 30 mm (W x H x D) without Antenna
EMI:	FCC Class B, CE Mark B,

Limited Warranty

TRENDnet warrants its products against defects in material and workmanship, under normal use and service, for the following lengths of time from the date of purchase.

Wireless	Three years
----------	-------------

If a product does not operate as warranted above during the applicable warranty period, TRENDnet shall, at its option and expense, repair the defective product or deliver to customer an equivalent product to replace the defective item. All products that are replaced will become the property of TRENDnet. Replacement products may be new or reconditioned.

TRENDnet shall not be responsible for any software, firmware, information, or memory data of customer contained in, stored on, or integrated with any products returned to TRENDnet pursuant to any warranty.

There are no user serviceable parts inside the product. Do not remove or attempt to service the product through any unauthorized service center. This warranty is voided if (i) the product has been modified or repaired by any unauthorized service center, (ii) the product was subject to accident, abuse, or improper use (iii) the product was subject to conditions more severe than those specified in the manual.

Warranty service may be obtained by contacting TRENDnet office within the applicable warranty period for a Return Material Authorization (RMA) number, accompanied by a copy of the dated proof of the purchase. Products returned to TRENDnet must be pre-authorized by TRENDnet with RMA number marked on the outside of the package, and sent prepaid, insured and packaged appropriately for safe shipment.

WARRANTIES EXCLUSIVE: IF THE TRENDNET PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT TRENDNET'S OPTION, REPAIR OR REPLACEMENT. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. TRENDNET NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF TRENDNET'S PRODUCTS.

TRENDNET SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR OR MODIFY, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: TO THE FULL EXTENT ALLOWED BY LAW TRENDNET ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT TRENDNET'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

Governing Law: This Limited Warranty shall be governed by the laws of the state of California.

Note: AC/DC Power Adapter, Cooling Fan, and Power Supply carry 1-Year Warranty



TRENDnet Technical Support

US • Canada

Toll Free Telephone: 1(866) 845-3673

24/7 Tech Support



Europe (Germany • France • Italy • Spain • Switzerland • UK)

Toll Free Telephone: +00800 60 76 76 6

WorldWide

Telephone: +(31) (0) 20 504 05 35

English/ Espanol - 24/7

Francais/ Deutsch - 11am-8pm, Monday - Friday MET

Product Warranty Registration

Please take a moment to register your product online.

Go to TRENDnet's website at <http://www.trendnet.com>

TRENDnet
3135 Kashiwa Street
Torrance, CA 90505
USA